Appendix D

VALIDATION, VERIFICATION, AND ACCREDITATION
A PERSPECTIVE FROM THE INTELLIGENCE COMMUNITY

Betsy Stone Witt, National Air Intelligence Center
Aerodynamic Weapons Design Branch

INTRODUCTION

Verification, validation, and accreditation (VV&A) of digital models have become an issue of concern to the military operations research community. This paper presents National Air Intelligence Center (NAIC) philosophies on VV&A of the representation of threat weapon systems in digital models. To illustrate the concepts, a sample VV&A effort is provided.

BACKGROUND

NAIC subscribes to the MORS definitions of verification, validation, and accreditation:

> **Verification**: The process of determining that a model implementation accurately represents the developer's conceptual description and specifications.
>
> **Validation**: The process of determining the degree to which a model is an accurate representation of the real world from the perspective of the intended uses of the model.
>
> **Accreditation**: An official determination that a model is acceptable for a specific purpose.

In the intelligence community, we place special emphasis on the phrases "...from the perspective of the intended uses of the model", and "...for a specific purpose", and find these phrases critically important to our VV&A. We further interpret the words "model" and "accuracy". In using the word "model", it is important to differentiate between a simulation program and a threat model. A "simulation program" models the behavior of physical systems. A "threat model" is the collection of specific data and source code that, together with a simulation program, represents the behavior of a particular threat system. The user of either must understand that VV&A of a simulation program do not validate a threat model constructed using that simulation program. Also, VV&A of one threat model may not validate another threat model, even using the same simulation program. Validation of a threat model can only be done using "intelligence" data.

It is also important to understand what accuracy means to threat models. While “accuracy” in the mathematical sense is established rigorously through probabilistic means, often in the intelligence community we label our models accurate if they are the best possible point design based on all available intelligence data. However, we acknowledge the best possible point design may not be acceptable for a specific purpose, as it may not be accurate enough in a probabilistic sense.

Threat Models Built Using Intelligence Data

Intelligence modelers often have imperfect knowledge of the inputs to the model, and make estimates as needed to ensure the performance of the model matches what is generally believed to be the capability of the threat system. That is, if we say that the equation A + B = C is valid, because A and B in fact add up to C, and we can validate C, we may not be stating that A and B are valid. So A may be high, and B may be low, but since their sum works out to be C, we know we have a good model, at least if C is the parameter of interest in the particular application. (If A or B are of interest, we must supply information on our confidence in these parameters). Because of this, a threat model may not lend itself to piecemeal, or functional level validation. Sensitivity analysis may be difficult with threat models (models built using intelligence data) since errors in input parameter values may be interdependent. No single parameter can be varied independently because its assessed value in general is correlated with other model parameters in order that observed constraints -- the real world -- be matched. In intelligence modeling, the “real world” means any and all actual data available on the system or its subsystems.

VV&A from the Intelligence Community Perspective

Verification: The system and subsystem are continually tested and exercised in appropriate scenarios to convince the developer the system or subsystem being modeled is behaving as intended. For example, if control fin deflection are being modeled, the developer might command the missile to turn right, turn left, climb, dive, and use combinations of these maneuvers to assure the actuators are operating as expected and the fins are responding in kind. This kind of testing takes place all throughout model development, for every conceivable subset of the complete system. Thousands of tests may be run before a modeler “has it right”. Other engineers are often consulted.

Validation: Also taking place throughout a model’s development are rigorous comparisons to any and all “real data” that are available on the system and subsystems being modeled. “Known” data take precedence in a model. Other parameters may be manipulated so that “known” data values are achieved. If performance data are known, the model must be built to deliver same. Known-data inconsistencies are resolved and explained using engineering judgment and interdata correlation. When these models are finished they are the best possible based on all available information.

Accreditation: The customer or model user is the accreditor. When a model is finished, the customer must determine if the model satisfies accuracy and performance requirements. If shortcomings are noted, further development is possible; however, in the case of intelligence models, this generally means certain elements within the model will be interpolated or extrapolated, since the model has already been defined to match all available real world data. Any changes made to the model must not invalidate model performance as dictated by available real world data.

TRAP - A VV&A Example

TRAP is a simulation program that supports the design and performance evaluation of threat air-launched weapons. Used by NAIC for about 15 years, the program and its threat model database are exported to many tri-Service users and their contractors. Verification and validation of TRAP digital threat models are done by the developer (NAIC) throughout a model's development cycle, while the application-dependent user-accreditation takes place when the customer is ready to use it for some purpose.

In 1991, the Air Force Intelligence Support Agency (AFISA) (now the 497th Intelligence Group), examined parts of the TRAP 3.0 library code. Though the program version now has been superseded, their findings, summarized in the executive summary of their final report, illustrate what might be expected from similar efforts:

> "TRAP 3.0 provides a high-fidelity simulation of the basic missile aerodynamics. It could improve its representation of non-symmetrical bank-to-turn missiles. This would increase its analytical capability for many anti-ship and air-launched cruise missiles. The fact that TRAP 3.0 does not model advanced seeker....capabilities limits the model's usefulness for analyzing advanced weapons systems engagements... Its end-game computations must be treated carefully because it does not model missiles fuzing or the change in missile center-of-gravity *(ed. note: this is untrue)*. TRAP 3.0's flyout computations are adequate to determine missile kinematics during engagement. They, however, do not always provide enough resolution for accurate intercept determinations. TRAP 3.0 provides adequate simulation for conventional (i.e., current) countermeasures, but cannot model random guidance errors possibly introduced by directed energy weapons.
>
> TRAP 3.0's low-fidelity simulation of launch and target aircraft is adequate for mid- to high- altitude engagements, but lacks the advance radar modeling needed for low-level look-down/shoot-down scenarios. Also, because of its limitations in radar modeling, TRAP probably does not provide accurate results for engagements involving reduced radar signature weapons systems... It does not model aircraft thrust vectoring, (though it can model missile thrust vectoring) nor does it have the capability to investigate high angle-of-attack missile launch scenarios. This limits evaluating enhanced launch envelopes.
>
> We recommend the continued use of TRAP 3.0 for missile performance analysis of medium-to-high altitude engagements that employ only conventional countermeasures. However, incorporating TRAP 3.0 into a larger model designed to evaluate more realistic engagements, especially those that investigate low-level intercept, requires several modifications to the air intercept radar, missile seeker (active), and missile/aircraft aerodynamics (thrust vectoring capabilities and high-alpha maneuvers). FASTC *(now NAIC)* threat models of currently-deployed CIS missiles will provide realistic results using accepted engagement tactics. However, threat models of missiles with more sophisticated fully-active radar as will lack the range and Doppler capabilities to model target tracking through interference." **(The simulation has undergone many upgrades since this report).*

High Fidelity Models vs. Low Fidelity Models

High fidelity models strive to accurately represent a threat system's kinematic (flight trajectory, miss distance, sensor mechanics) and electronic (sensing and guidance and control system) capabilities. They are supported by excellent data availability, both in quality and quantity. In intelligence modeling, if a high fidelity model can be supported, we build one. However, data availability may preclude the production of a high fidelity model. In these cases a low fidelity model is built, but is still the best possible based on the available information.

Not all applications require or support high fidelity modeling. A lower fidelity model can be extracted from the high fidelity model and made to yield the same performance results in the user's application space. For example, in benign environment intercepts, low and high fidelity models may yield approximately the same miss distance; however, "edge-of-the-envelope" (close-in, highly maneuverable, countermeasures dependent) performance may be significantly more accurate if generated using a high fidelity model.

SUMMARY

This paper has provided the operations research community with some insight into the world of intelligence modeling, highlighted the challenges of threat model VV&A, and illustrated that certain facets of VV&A are an integral part of model development. NAIC will continue to place a high priority on responding to the needs of the acquisition and operational customer for validated, verified digital threat models.

BIOGRAPHY

Betsy Stone Witt has a B.S. and M.S. in Mathematics, and has done air-launched weapons design, performance, and engagement analysis at the National Air Intelligence Center (formerly the Foreign Aerospace Science and Technology Center, Foreign Technology Division) for 16 years. She is a specialist in building software simulations of hardware systems, and currently creates high fidelity digital models of air-to-air missiles.